MULTIMEDIA OUTPUT DEVICE HAVING EMBEDDED ENCRYPTION FUNCTIONALITY

Inventors:
Jonathan J. Hull
Michael J. Gormish
Kurt W. Piersol

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] The present application claims priority under 35 U.S.C. § 119(e) to the following provisional patent applications, each of which is incorporated by reference in its entirety: U.S. Provisional Application Serial No. 60/506,303, filed September 25, 2003, and titled "Printer Including One or More Specialized Hardware Devices" and U.S. Provisional Application Serial No. 60/506,302, filed September 25, 2003, and titled "Printer Including Interface and Specialized Information Processing Capabilities."

[0002] This application is a continuation-in-part and claims priority from the U.S. Patent Application No. 10/639,282, titled "Physical Key For Accessing a Securely Stored Digital Document", filed August 11, 2003, the disclosure of which is incorporated by reference.

BACKGROUND

Field of the Invention

[0003] This invention relates generally to multimedia output devices that have embedded encryption functionality, and in particular to methods and systems that encrypt content

and provide electronic output and associated paper output that provides information about the decryption.

Background of the Invention

[0004] Frequently, users need to maintain security of electronic data. Data encryption is one of the most effective ways to achieve data security. To read an encrypted file, one needs to have access to a key or password that enables a user to decrypt the file. A one-time pad algorithm is a well-known encryption algorithm used by some very secure encryption systems. According to this technique, the decryption key is of the same length as the data that needs to be encrypted. As a result, this technique presents difficulties for users because they cannot remember long strings of random characters.

[0005] Alternative solutions to using the one-time pad algorithm are known. One solution requires users to provide their own passwords that are used to encrypt data. However, user-provided passwords are often vulnerable to password cracking techniques.

[0006] Another solution requires users to register with some authority, such as a public-key authority, to set up a public-private key pair used to encrypt and decrypt the data. However, most people do not have time to set up such keys.

[0007] To overcome the limitations of existing encryption techniques, it has been known to embed encryption functionality in computing devices. These computing devices are adapted to generate keys used to encrypt or decrypt data. To produce a paper output of the generated key, these devices need to send instructions to a printer or other output device. In addition, if a user desires to create multiple copies of the encrypted data, the computing device needs to be equipped with a plurality of removable media devices.

Thus, if a user desires to have multiple copies of the encrypted data in the electronic format as well as a paper output of the generated key, a user needs to have at least a computing device having encryption functionality, a printer, and a device capable of writing encrypted data to multiple removable media devices.

[0008] Furthermore, existing computing devices that embed encryption functionality do not generate separate keys for each encrypted data. This is undesirable because it reduces the security of the system because multiple encrypted data would share the same key.

[0009] Accordingly, what is needed is a device that embeds the encryption functionality of the conventional computing device without the limitations of conventional techniques for outputing decryption information.

SUMMARY OF THE INVENTION

[0010] A multimedia output device having embedded encryption functionality enables the outputting of content in an encrypted form. The multimedia output device receives the content, encrypts the content, and provides an electronic output of the encrypted content. In certain embodiments, the multimedia output device also generates an associated paper output that provides information about the encryption, such as a decryption key, an identification of the electronic output of the encrypted content, and optionally a description of the content. The separation of the decryption key from the encrypted content provides security for the encrypted content since the key is stored separately from the encrypted content. If the encrypted content fell into unauthorized hands, an unintended recipient would not have the key to decrypt the content.

[0011] In one embodiment, a multimedia output device includes an interface for receiving content, such as audio or video content, and a content processing system coupled to the interface to receive the content. The content processing system, in turn, includes an encryption module that performs the encryption functionality. In one embodiment, the encryption module generates a key and encrypts the content using the generated key. In another embodiment, the encryption module encrypts the received content using a key provided by the user. The encryption module executes a key and metadata generation module, which is adapted to receive unencrypted content and to generate various levels of description of the content in response to a user's selection of a security level. Such a description includes keywords, key frames from a video, or just a title. Thus, a low security level would result in a description containing meaningful

keywords or key frames while a high security level would result in a printed description that revealed less about the content. In one embodiment, the key and metadata module is further adapted to generate decryption information, which includes a generated key, an identifier of the electronic output of the encrypted content, and description of the encrypted content.

[0012] The multimedia output device also includes an electronic output system adapted to receive the encrypted content and produce a corresponding electronic output. The multimedia output device also includes a printing output system in communication with the processing system. The printing output system receives decryption information from the key and metadata module and generates an associated paper output that provides information about the decryption.

[0013] The multimedia output device also includes a user interface that provides to a user a selection of the options in connection with data encryption. Such options include the type of encryption desired, the output format of the encrypted content, and the output format of the decryption information. Various encryption techniques include symmetric encryption, a public key encryption, and symmetric encryption with the key encrypted with a recipient's public key. The choices of the output format for the encrypted data and for decryption information include an electronic format and a paper format. Additionally, the user interface allows a user to choose the level of security at which decryption information will be provided.

[0014] Additional embodiments of the invention provide for encryption of audio and video data. To this end, the key and metadata module is adapted to perform various

levels of processing of audio and video data, such as producing a transcript and extracting keywords from audio data, extracting key frames from video data and printing them on paper along with bar codes. A user is allowed to choose the level of security with which the decryption information should be printed. The encryption module, in turn, is adapted to encrypt audio and video data using various encryption algorithms for encrypting audio and video data.

[0015] Additional embodiments of the multimedia output device provide for receiving content, encrypt the content using a user's private key, and outputting the encrypted content that can be decrypted using a user's public key. This embodiment is beneficial because it provides the ability for a recipient to authenticate the content. The content can be both encrypted and signed, to provide security and authentication.

[0016] Additional embodiments of the invention provide for decryption of encrypted content. Multimedia output device is adapted to receive encrypted content and a key used to decrypt the content. Multimedia output device decrypts the content using well-known techniques and generates an electronic output of the decrypted content. In addition, the multimedia output device is adapted to process the decrypted content and to produce a summary, which is outputted on any medium selected by a user.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIG. 1A is a schematic diagram of a system in accordance with an embodiment of the invention.

[0018] FIG. 1B is a schematic diagram of an embodiment of the system shown in Fig. 1A that performs decryption of encrypted content.

[0019] FIG. 2A is a user interface for selecting an electronic format and security level of a paper output in accordance with an embodiment of the invention.

[0020] FIG. 2B is an example of a paper output of decryption information in accordance with an embodiment of the invention.

[0021] FIG. 2C is an example of a paper output of decryption information in accordance with another embodiment of the invention.

[0022] FIG. 2D is an embodiment of system 100 in which decryption information is provided in a paper format.

[0023] FIG. 2E is an embodiment of system 100 in which decryption information is provided in an electronic format.

[0024] FIG. 3 is a schematic diagram of various processing systems of the multimedia output device in accordance with embodiments of the present invention.

[0025] FIG. 4A is a flow diagram of the process performed by the multimedia output device in accordance with one embodiment of the present invention.

[0026] Fig. 4B is a flow diagram of the process performed by the multimedia output device in accordance with another embodiment of the present invention.

[0027] FIG. 5 is a block diagram of functional modules of encryption module in accordance with one embodiment of the present invention.

[0028] FIG. 6 is a flow chart of the embodiment in which symmetric key encryption is used.

[0029] FIG. 7A is a flow chart of the embodiment in which public key encryption is used.

[0030] FIG. 7B is a flow chart of the embodiment in which content is encrypted using a user's private key.

[0031] FIG. 8 is a flow chart of the embodiment in which symmetric key is encrypted with a public key.

[0032] FIG. 9 is a flow diagram of the embodiment in which multiple keys are generated.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0033] Various embodiments of a multimedia output device 120 having embedded encryption functionality enable the outputting of content in an encrypted form. Certain embodiments also output an associated paper output that provides information about decryption, such as a decryption key, an identification of the electronic output of the encrypted content, and description of the content encrypted. Depending on the desired application for the multimedia output device 120, the multimedia output device 120 includes any number of devices for receiving the content, outputting the paper output, and producing the electronic output.

Overall System Architecture

[0034] Fig. 1A is a high-level diagram of one embodiment of a system 100 in accordance with the present invention. System 100 includes a multimedia output device 120 capable of receiving content 150 to be encrypted and providing an electronic output 170 of the encrypted content and an associated output 160 that provides information about decryption. In some embodiments, output 160 is printed on paper. In other embodiments, output 160 is written to a digital medium. In still other embodiments, output 160 is displayed on a display screen. In an alternative embodiment, device 120 is adapted to output encrypted content and information about decryption serially onto a single output medium. For example, device 120 outputs encrypted content onto a digital medium and then outputs decryption information onto the same medium.

[0035] Content includes one or a combination of audio (including music, radio broadcasts, recordings, advertisements, etc.), video (including movies, video clips,

television broadcasts, advertisements, etc.), software (including video games, multimedia programs, graphics software, etc.), pictures (including jpeg, jpeg2000, gif, tif, etc.) and documents (including Postscript, PCL, pdf, Word, etc.). This listing, however, is not exhaustive. Content may be encoded in any format or encoding technology, including Moving Pictures Experts Group (MPEG-2) format for video and MPEG-3 (mp3) for audio.

[0036] Multimedia output device 120 receives unencrypted content 150, encrypts the received content, and produces an electronic output of the encrypted content in any desired format. Multimedia output device 120 also outputs output 160 providing information about decryption of the content.

[0037] Multimedia output device 120 receives unencrypted content 150 from various sources, as will be discussed in greater detail in reference to Fig. 3. The multimedia output device 120 uses a variety of encryption algorithms to encrypt content 150, such as triple Data Encryption Standard (DES) algorithm, symmetric key encryption, one time path, public key encryption, encryption using symmetric key with further encryption of the symmetric key with a user's public key, and encryption using symmetric key with further encryption of the symmetric key using the recipient's public key.

[0038] The multimedia output device 120 writes the electronic output 170 of the encrypted content to a media device, such as a writeable DVD or CD, a video cassette tape, an audio cassette tape, a flash card, a computer disk, an SD disk, a memory stick, or any other appropriate electronically-readable medium. The encrypted data can be

transmitted over a network, written to a memory device via USB or IEEE 1394. The encrypted content can also be printed to paper.

[0039] The multimedia output device 120 also outputs an associated output 160 that provides information about the decryption, such as the key "F54jk890XC" 270, an identification of the electronic output of the encrypted content, such as "DVD number 45378" 260 (as shown in Fig. 2B). The decryption information optionally includes a description of the content. This information will be used by the intended recipient of the encrypted content to decrypt the data. As used herein, the word "key" means a password, data, or a table used to decrypt encrypted data. In alternative embodiments, the decryption information is provided in an electronic format separately from the encrypted content.

[0040] The separation of the key from the encrypted content provides security for the encrypted content since the paper or any other medium containing the key is stored separately from the encrypted content. If the encrypted content fell into unauthorized hands, the unintended recipient would not have the key to decrypt the data. Accordingly, the loss of the output 160 that includes the decryption information does not affect the security of the electronic output 170 as long as both the output 160 and electronic output 170 do not fall into the unauthorized hands.

[0041] It should be noted that a user is allowed to provide a selection of the options in connection with data encryption. Such options include the type of encryption desired, the output format of the encrypted data, and the output format for the encryption data, as will be described in more detail below in reference to Fig. 2A.

[0042] The multimedia output device 120 preferably includes any necessary subsystem, as known by one skilled in the art, to print on a printable medium, such as a sheet of paper. Although outputting on paper is discussed above, it should be understood that a multimedia output device in accordance with various embodiments of the present invention could produce an image, words, bar codes, or other markings onto a variety of media, such as transparency sheets for overhead projectors, film, slides, canvas, glass, stickers, or any other medium that accepts such markings.

[0043] Depending on the intended application, multimedia output device 120 takes many different forms other than the typical office or home-use multimedia output device with which most people are familiar. Therefore, it should be understood that the definition of the multimedia output device 120 includes any device that is capable of producing an image, words, or any other markings on a surface.

[0044] Fig. 1B is a high-level diagram of the system shown in Fig. 1A, in which multimedia output device 120 is adapted to receive encrypted content 171 and a key (not shown) used to decrypt the content 171 and to produce decrypted electronic output 172 and/or decrypted paper output 174. It should be noted that encrypted content 171 could be encrypted output 170 generated by device 120. Alternatively, encrypted content 171 is any encrypted content provided by a user. A key can be provided to device 120 via a keyboard, scanning a bar code, or using any known optical content recognition (OCR) technique with a key printed on paper or provided electronically by a driver software.

[0045] It should be noted that multimedia output device 120 is adapted to decrypt encrypted content 171 using any well-known decryption technique. The multimedia

output device 120 is adapted to perform further processing of the decrypted content to produce a summary of the content. Such a summary could be outputted onto any medium specified by a user.

User Interface

[0046] Fig. 2A illustrates an exemplary user interface (UI) 200 for selecting various options in connection with encryption functionality embedded into multimedia output device 120. For example, a user is allowed to choose the type of encryption desired, the output format of the encrypted data, the output format for the decryption information, and a desired security level at which information about the decryption should be outputted.

[0047] The UI 200 is preferably displayed on a screen on which information is conveyed to the user. UI 200 preferably also includes a mechanism for allowing a user to input responses and make selections. In one embodiment, the UI 200 includes a touch screen 206, which allows the user to make selections and inputs by touching an appropriate part of the screen. In one embodiment, a keypad is also provided for entry of alphanumeric data. In an alternative embodiment, a joystick, trackball or other input device is used to provide input and make selections. It should be noted that in alternative embodiments, the user's input is provided via a multimedia output device driver dialog box on any client device or via a web page that sends data to multimedia output device 120 via secure HTTP or some other network protocol. As used herein, the "client device" is any wired or wireless device, including, but not limited to PDAs, cell phones, and stand alone computer systems.

[0048] As shown in Fig. 2A, UI 200 presents a user with a choice of the type of encryption desired. Such choices include symmetric encryption 212, public key encryption 214, and encryption using symmetric key with further encryption of the symmetric key using a recipient's public key 216. It should be noted that a recipient could be a user or any other intended recipient. These methods will be described in greater detail below. Screen 206 of UI 200 includes an instruction to the user to "select type of encryption." If a user selects the public key encryption method or symmetric encryption method with symmetric key encrypted with a recipient's public key, the user is provided with an option of entering his public key or the intended recipient's public key. Optionally, a user is allowed to choose the length of the key that will be used to decrypt the encrypted content. In addition, a user is allowed to edit the content before it is encrypted.

[0049] The UI 200 also allows a user to choose an output format for the encrypted content. Such choices include, for example, providing the encrypted content in an electronic format or in a paper format. As discussed above, the choices of the electronic formats presented to a user include, but are not limited to, removable storage devices, such as a writeable DVD or CD, a video cassette tape, an audio cassette tape, a computer disk, a SD disk, a USB drive, or any other appropriate electronically-readable medium. In the illustrated embodiment, the user selects from DVD 220, CD 222, SD 224, USB 226, File 228, and email 230. These options are shown by way of an example only. Those skilled in the art will appreciate that the present invention may be applied to any other output format that exists or may exist in the future.

[0050] The UI 200 optionally allows a user to select an output format for the decryption information (not shown). Such choices include providing the decryption information in an electronic format or in a paper format. The choices of the electronic formats presented to a user include, but are not limited to, removable storage devices, such as a writeable DVD or CD, a video cassette tape, an audio cassette tape, a computer disk, an SD disk, a USB drive, or any other appropriate electronically-readable medium.

[0051] In addition, the UI 200 allows the user to select a desired security level at which information about the decryption should be outputted. The embodiment of Fig. 2A shows ten security settings for selecting a paper security level. Ten security settings (1-10) are referenced by legend numbers 232-250 respectively. UI 200 includes several selections for the user to choose from. In the illustrated embodiment, a user is allowed to select a desired security level by checking an appropriate box. It should be noted that a user's choice of the level of security is based on the user's desire to trade off security and utility of the paper output. In one implementation, when the user selects the most secure (level 10), the generated output 160 identifies only the electronic output 170 of the encrypted data and the key that decrypts the content. When the user selects a less secure paper representation of decryption information, such as level 9, the output 160 includes, for example, a short description of the encrypted content, such as the date and title of the content.

[0052] Fig. 2B, illustrates an example paper output 160a of decryption information in accordance with one embodiment. In the illustrated embodiment, the paper output 160a is shown in response to a user selection of the security level 10 and "DVD" as an

electronic format for the encrypted content. The paper output 160a provides minimum required information to decrypt the encrypted content 150. Output 160a, for example, provides an identifier 260 of the electronic output of the encrypted content, such as "DVD number 45378" and the key 270 that decrypts the content, such as "F54jk890XC."

[0053] Fig. 2C, illustrates an example paper output 160b of decryption information in response to a user selection of the security level 9 and "DVD" as an electronic format for the encrypted content. In the illustrated embodiment, the paper output 160b provides a less secure paper representation of encrypted information than the one shown in Fig. 2B. Such a printout additionally includes information, such as the date 280 and title 290 of the content. Although this description is less secure, it has more utility because it describes the encrypted content with greater particularity.

[0054] Fig. 2D is an embodiment of system 100 in which decryption information is provided in the form of a paper output. Fig. 2D shows two paper outputs 160a and 160b of Figs. 2B and 2C. Output 160a provides decryption information in response to a user choosing the most secure level of security (level 10) of outputting decryption information. Output 160b provides decryption information in response to a user choosing a less secure level (level 9). As shown in Fig. 2D, encrypted content is provided in the electronic format, such as a writeable DVD 170.

[0055] Fig. 2E shows an alternative embodiment of system 100. In this embodiment, decryption information is stored in the electronic format, such as on a writeable DVD 160. When a one-time pad algorithm is used to encrypt content, the key used to decrypt the content has a long string of characters. Accordingly, outputting decryption

information in the electronic format beneficially allows a user to store the long string of characters of the decryption key. In alternative embodiments, decryption information could be outputted on any type of non-volatile storage medium. The decryption information can also be emailed to a user or could be displayed on a UI 200.

Architecture of Multimedia Output Device

[0056] Fig. 3 is a block diagram of one embodiment of multimedia output device 120. Multimedia output device 120 includes a source interface 305, a user interface 200, a printing output system 315, an electronic output system 320, and a content processing system 325. Capable of receiving content 150, the source interface 305 takes a variety of forms and includes one or more devices that receive content or create content by observing a content event. Similarly, the printing output system 315 and the electronic output system 120 take a variety of forms and each includes one or more devices that produce, respectively, an output 160 (printed or electronic) and an electronic output 170. Various components of multimedia output device 120 are further described in co-pending U.S. patent application entitled, "Printer Having Embedded Functionality for Printing Time-Based Media," to Hart et. al., filed March 30, 2004, Attorney Docket 20412-8340, which application is incorporated by reference in its entirety.

[0057] The user interface 200 has been described above in reference to Fig. 2A. The user interface 200 includes a display system, software for communicating with an attached display, or any number of embodiments described in co-pending U.S. patent application entitled, "Printer User Interface," to Hart et. al., filed March 30, 2004, Attorney Docket No. 20412-08455, which application is incorporated by reference in its entirety. The

content processing system 325 is coupled to the source interface 305 and the user interface 200. The content processing system 325 is also coupled to the printing output system 315 and to the electronic output system 320 for providing the appropriate commands and data to those systems.

[0058] The content processing system 325 includes a processor 335 and a memory 330. Content processing system 325 also includes an encryption module 340. The encryption module 340 is adapted to receive content from various sources and to encrypt the received content. The encryption module 340 includes software, hardware, or a combination thereof for implementing an encryption functionality of multimedia output device 120.

[0059] The electronic output system 320 receives the encrypted content and generates an electronic output of the encrypted content, as described above in reference to FIG. 1A. In one embodiment, multimedia output device 120 writes the electronic output to a media device with a media writer (not shown). The media devices includes, for example, a removable storage devices such as a writeable DVD or CD, a video cassette tape, an audio cassette tape, a flash card, a computer disk, an SD disk, a memory stick, or any other appropriate electronically-readable medium. The media writer is further adapted to attach a unique identification of the encrypted content to a removable storage device that stores the encrypted content. Such identification, for example, includes a combination of alphanumeric characters.

[0060] The printing output system 315 produces an associated printed output of the decryption information. Such printed information includes, for example, a decryption key, an identification of the electronic output of the encrypted content, and optionally a

description of the contents encrypted. The printing output system 315 comprises any standard printing hardware, including the one that is found in standard laser multimedia output devices, inkjet multimedia output devices, thermal wax transfer printers, dot matrix printers, and other printers as are known in the art.

[0061] Multimedia output device 120 includes an embedded Audio/Video (A/V) content recognition module 370 that performs one or more of video event detection, video foreground/background segmentation, face detection, face image matching, face recognition, face cataloging, video text localization, video optical character recognition (OCR), language translation, frame classification, clip classification, image stitching, audio reformatting, speech recognition, audio event detection, audio waveform matching, caption alignment, audio-caption alignment, and any other type of content recognition algorithms.

[0062] Multimedia output device 120 also includes a control module (not shown) that allows a user to edit the input content before it is encrypted. It should be noted that the control module is adapted to reside on the device associated with a user or on some other external device.

[0063] Various embodiments of multimedia output device 120 having audio/video content recognition are described in a co-pending U.S. patent application entitled, "Printing System With Embedded Audio/Video Content Recognition and Processing," to Hull et. al., filed March 30, 2004, Attorney Docket No. 20412-08394, which application is incorporated by reference in its entirety.

Content Source Interface

[0064] Fig. 3 further illustrates some examples of external sources from which multimedia output device 120 receives content 150. Depending on the desired input, the interface 305 allows the multimedia output device 120 to communicate with a wide variety of different electronic devices that can provide the multimedia output device 120 with content to print. Without intending to limit the types of devices, the interface 305 allows the multimedia output device 120 to receive content from external sources such as computer systems, computer networks, digital cameras, video cameras, media renderers (such as DVD and CD players), media receivers (such as televisions, satellite receivers, set-top boxes, radios, and the like), external storage devices, video game systems, or any combination thereof. The connection type for the interface 305 takes a variety of forms based on the type of device that is intended to be connected to the multimedia output device 120 and the available standard connections for that type of device. For example, the interface 305 comprises a port for connecting the device using a connection type such as USB, serial, FireWire, SCSI, IDE, RJ11, optical, composite video, component video, or S-video, or any other suitable connection type. The interface 305 can be a wireless interface that allows the multimedia output device 120 to receive content from a wireless device external to the multimedia output device 120. The interface 305 can allow the multimedia output device 120 to communicate with any number of wireless communication systems, such as wireless components on a home or business network, cellular phones and other portable wireless devices, satellites, satellite dishes, and devices using radio transmissions. Depending on the types of external devices with which the

multimedia output device 120 is desired to communicate, the interface 305 comprises hardware and/or software that implements a wireless communications protocol, such as that described in IEEE 802.11 or the Bluetooth standard.

[0065] In another embodiment, the multimedia output device 120 receives content from a removable media storage reader 360 that is built into the multimedia output device 120. The removable media storage reader 360 is configured to accommodate any type of removable media storage device, such as DVDs, CDs, video cassette tapes, audio cassette tapes, floppy disks, ZIP disks, flash cards, micro-drives, memory sticks, SD disks, scanners, pdf machines, or any other suitable type of media storage devices. Moreover, the multimedia output device 120 is configured to include a plurality of removable media storage readers 360 to accommodate multiple types of media storage devices.

[0066] In another embodiment, the multimedia output device 120 includes an embedded video recorder (not shown in Fig. 3). In this embodiment, the external source of content is a series of images captured by the embedded video recorder. The video recorder, such as a camera, CCD, or other suitable mechanism for capturing a sequence of images, converts a scene into a suitable electrical format, such as that described in the MPEG, H.263, or H.264 standards.

[0067] In another embodiment, the multimedia output device 120 includes an embedded audio recorder (not shown in Fig. 3). In this embodiment, the external source of content is a series of sounds that are converted into a digital format by the embedded audio recorder. The audio recorder converts the recorded sound signal into a suitable electrical format, such as MPEG-2.

[0068] In another embodiment, the multimedia output device includes video capture hardware (not shown). In one embodiment, the video capture hardware is designed to be coupled to a computing system by a video cable thereof. The video cable from a display is attached to the multimedia output device 120, where the video signal is split with one signal directed to the computing system and another signal to the video capture hardware. The video capture hardware performs a differencing between successive frames of the video signal and saves frames with a difference that exceeds a threshold on a secondary storage in the multimedia output device 120. This offloads such processing from the computing system, thereby improving responsiveness and user experience and providing an easily browseable record of a user's activities during the day.

[0069] Various components of multimedia output device 120 and various content sources are further described in co-pending U.S. patent applications, each of which is incorporated by reference in its entirety: U.S. Patent Application entitled, "Printer Having Embedded Functionality for Printing Time-Based Media," to Hart et. al, filed March 30, 2004, Attorney Docket 20412-8340 and U.S. Patent Application entitled, "Networked Printing System Having Embedded Functionality for Printing Time-Based Media," to Hart et. al, filed March 30, 2004, Attorney Docket 20412-8341.

Methods of Operation

[0070] FIG. 4A is an overview of a generalized process by which the multimedia output device 120 creates an encrypted representation of the content and paper representation of decryption information in accordance with one embodiment of the present invention. It should be noted that methods related to various types of encryption techniques utilized by

multimedia output device 120 are described in more detail below in reference to Figs. 6-8.

[0071] The process starts 405 and the multimedia output device 120 receives 410 content from an external source. This content is received as digital or analog content, or it may be an observable event that interface 305 records as digital or analog data. Encryption module 340 encrypts the received content 420 according to, for example, a known encryption algorithm. Multimedia output device 120 provides 430 an output of the encrypted content. As described above, the encrypted content is outputted in an electronic format or in a paper format, as desired by a user. Multimedia output device 120 also provides 440 an output of the decryption information, such as a decryption key, identification of the electronic output of the encrypted content, and optionally contents. It should be noted that in an alternative implementation, the decryption key is outputted as a bar code. The decryption information is outputted on a paper or in an electronic format.

[0072] Fig. 4B is a flow diagram of a generalized process by which the multimedia output device 120 generates a decrypted representation of the content in accordance with one embodiment of the present invention.

[0073] The process starts 450 and the multi-media output device 120 receives 460 encrypted content. It should be noted that the encrypted content can be encrypted output 170 generated by multimedia device 120. Alternatively, encrypted content can be any content provided by a user that has been encrypted by other means than device 120. The multimedia output device 120 receives a key used to decrypt the encrypted content. As previously described, the key can be provided using various techniques, such as via a

keyboard, or scanning a bar code, or using OCR with a key printed on paper, or alternatively, the key provided electronically.

[0074] Encryption module 340 decrypts 470 the content according to, for example, a known decryption algorithm. Multimedia output device 120 provides 480 an output of the decrypted content. The decrypted content is outputted, for example, in an electronic format, or a network interface, or in a paper format, as desired by a user.

Encryption Module Architecture

[0075] Fig. 5 is a block diagram of functional modules of encryption module 340 in accordance with one embodiment of the invention. The encryption module 340 executes a random number generator module 510, a key and metadata generator module 520, a module 530 for executing encryption logic, and a module 540 for executin decryption logic. As used herein, the term "module" refers to program logic for providing the specified functionality that can be implemented in hardware, firmware, and/or software. In one embodiment, a software module is implemented with a computer program product comprising a computer-readable medium containing computer program code, which can be executed by a computer processor for performing the steps, operations, or processes described herein.

[0076] The random number generation module 510 is adapted to generate a random number and send the generated random number to the key and metadata generation module 520. Module 510 is a pseudo random number generator running on a microprocessor or a digital signal processor (DSP) designed for performing the logic

involved in digital signal processing. Module 510 is also adapted to generate a noise signal in order to provide a random number.

[0077] Module 520 is adapted to receive the random number generated by module 510. Module 520 generates a key using the provided random number and forwards the generated key to module 530. In one embodiment, when a public key encryption is utilized (as will be discussed below in reference to FIG. 7A), module 520 does not generate a key since a user knows his private key that will be used to decrypt the content.

[0078] Module 520 is also adapted to generate multiple keys for different parts of the content to be encrypted. Module 520 generates a unique identification that will identify the electronic output of the encrypted data. This identification will be used by the electronic output system 320 to attach the identification to a removable storage device that stores the encrypted content.

[0079] Module 520 is further adapted to receive a user selection of the security level with which decryption information should be provided. Module 520 is further adapted to receive unencrypted content and to perform an action in response to the received content and a user selection. Module 520 maintains rules indicating what action needs to be taken in response the user input and received content. Examples of these rules are shown below in Table 1. In one embodiment, performing an action includes generating decryption information. Decryption information includes, for example, a key, an identification of the electronic output of the encrypted content, and description of the received content. Module 520 uses well-known data extraction algorithms to generate various descriptions of the content in response to a user's desired choice of the security

level. Module 520 outputs the decryption information to the printing output system 315 or electronic output system 320 depending on the user's choice of the medium onto which decryption information should be provided. It should be noted that when a public key encryption method is utilized, generated decryption information does not include a key since the key is provided by a user.

[0080] Example rules maintained by module 520 are shown below in Table 1.

Table 1. Rules for Generating Decryption information

Security Level	Action
1	Generate transcript of the content Generate decryption information which includes: generated key, identification of the electronic output of the encrypted content; transcript of the content
...	...
7	Extract keywords from the content Generate decryption information which includes: generated key, identification of the electronic output of the encrypted content, and keywords
8	Extract key video frames; Generate decryption information which includes: Generated key, identification of the electronic output of the encrypted content, and Key video frames
9	Extract title and date of the encrypted content, Generate decryption information which includes: Generated key identification of the electronic output of the encrypted content, and Title and date of the encrypted content

10	Generate decryption information which includes: Generated key, and Identification of the electronic output of the encrypted content

A rule may be constructed such as:

IF (Security level (10))
THEN GENERATE IDENTIFICATION OF THE ELECTRONIC OUTPUT OF THE ENCRYPTED CONTENT AND KEY

[0081] Module 530 is adapted to receive the key generated by module 520. Alternatively, module 530 is adapted to receive a key from the user. Module 530 receives the content and encrypts the content using the provided key. Module 530 is adapted to encrypt the content using any of the known encryption algorithms, such as DES, IDEA, Blowfish, RSA, Triple DES, RC2 and RC4. Module 530 executes program logic for providing the encryption functionality that can be implemented in hardware, firmware, and/or software. Hardware designs known to perform the encryption are available from, for example, Amphion Semiconductor Ltd, of Belfast, Northern Ireland. These designs are listed below.

- CS5210 performs AES encryption using 128,192, or 256 bit keys
- CS5020 performs DES and triple DES encryption/decryption
- CS5312 performs SHA-2 encryption with key sizes of 256,384, or 512 bits

[0082] Hardware solutions, such as the one shown below, are also available, for example, from Eracom Technologies AG, of Krefeld, Germany:

- CSA8000 PKI-8PC/Server Encryption Adapter with RSA/DES in hardware

[0083] RSA (public key encryption) and Diffie-Hellman key generation algorithms are available in software development kits.

[0084] Software solutions to perform encryption are available from, for example, RSA Security Inc., of Bedford, MA. These solutions are designed to run on DSP chips. For example, Snapcrypt is a cryptographic library for the TMS320C54x and other TI DSPs.

[0085] Known encryption algorithms are specified in the following documents:

- DES is specified by ANSI X3.92 and FIPS 46-2, operation modes are specified in ANSI X3.106 and FIPS 81)
- Triple DES is specified in ANSI X9.52 and FIPS 46-3.
- SHA-1 is in ANSI X9.30-2 and FIPS 180-1.
- HMAC-SHA-1 is in IETF RFC 2104.
- MD5 is in IETF RFC 1321.
- DSA is in ANSI X9.30-1 and FIPS 186.
- Diffie-Hellman is in ANSI X9.42

[0086] It should be noted that in one embodiment, memory 330 maintains a log of keys generated by encryption module 340 so that the multimedia output device 120 can always re-print the key that was lost by the intended recipient. To increase the level of security, in one embodiment, the multimedia output device 120 maintains a list of symmetric keys encrypted with a user's public key. This method of encryption is described below.

[0087] Module 540 is adapted to receive a key and encrypted content, such as the content generated by encryption logic module 530 and to decrypt the received encrypted content using the key. Module 540 is adapted to decrypt the content using any of the known

decryption technique. Module 540 receives the key using any known technique, such as via a keyboard, scanning a bar code or using OCR with a key printed on paper. Module 540 is adapted to output decrypted content onto any medium specified by a user, such as an electronic medium, a network interface, or on paper.

Methods of Encryption

[0088] Fig. 6 is a flow chart of an embodiment of the present invention in which a symmetric encryption method is used. As is known in the art, symmetric encryption is a type of encryption in which the same key is used to encrypt and decrypt data. The process starts 605 and the multimedia output device 120 receives 610 content from an external source. Encryption module 340 generates a key 620 and encrypts 630 the received content using the key. The multimedia output device 120 then outputs 640 the encrypted data. The multimedia output device 120 also outputs the key that is used to decrypt the content.

[0089] Fig. 7A is flow chart of an embodiment of the present invention in which a public key encryption method is used. As is known in the art, public key encryption is a type of encryption that uses a public/private key pair. The process starts 705 and the multimedia output device 120 receives 710 content from an external source. Encryption module 340 receives 720 a public key from a user. In an alternative embodiment, a public key is provided from other sources. Encryption module 340 then encrypts 730 the received content using the key. The multimedia output device 120 then outputs 740 the encrypted data. A recipient of the encrypted data will use his private key to decrypt the data. It should be noted that this method does not provide an output of the decryption information

since the recipient already knows his own private key. The recipient needs to know his private key to decrypt the data.

[0090] Fig. 7B is a flow chart of an embodiment of the present invention in which content is encrypted using a user's private key. The process starts 750 and the multimedia output device 120 receives 760 content from an external source. Encryption module 340 receives 770 a private key from a user. In an alternative embodiment, a private key is provided from other sources. Encryption module 340 encrypts 780 the content using the private key, and outputs 790 encrypted content. The encrypted content is decrypted using a public key of a user. In an alternative embodiment, encryption module 340 runs a hash function on the received content and encrypts the hash with a user's private key. The hash function is a well-known cryptographic technique to provide a short sequence of bytes. In one embodiment, the encrypted hash is outputted along with the received content.

[0091] Fig. 8 is a flow chart of an embodiment of the present invention in which encryption module 340 generates a key, encrypts the content with the key, and encrypts the generated key with a recipient's public key. The process starts 805 and the multimedia output device 120 receives 810 content from an external source. Encryption module 340 receives 820 a public key from a user and generates 830 a symmetric key. It should be noted that if the encrypted data is intended for someone other than a user, the user provides the public key of the intended recipient. Module 340 then encrypts 840 the received content with the generated symmetric key. In step 850, module 340 encrypts the generated symmetric key with the received public key. The multimedia output device

120 then provides 860 an output of the encrypted information, including the encrypted symmetric key that will be used to decrypt the symmetric key. The multimedia output device 120 then outputs 870 the encrypted content separately from the key. To decrypt the content, a user would have to decrypt the symmetric key with his private key and then decrypt the content with the symmetric key. It should be noted that the above process can be repeated with several distinct public keys, each key received from a different user, so that the symmetric key is encrypted as many times as the number of the provided public keys. Generating individual outputs for a set of users allows each user to decrypt the content without the knowledge of another user's private key. This embodiment is utilized when documents need to be secure, yet shared among members of a group.

[0092] Fig. 9 is a flow chart of an alternative embodiment for encrypting the content. The process starts 905 and the multimedia output device 120 receives 910 content from an external source. Encryption module 340 generates 920 a key and encrypts 930 the content with the key. Encryption module 340 then generates 940 multiple fractional keys, each key containing a subset of the generated key. Fractional keys can be generated by any reversible method of decomposition which operates upon a sequence of bits. For example, a series of keys which will be combined bitwise by a Boolean XOR operation might be generated. Alternatively, the key could be divided bitwise into 2 or more contiguous sets of bits. Alternatively, an algorithm which divides the bit in some other way, such as choosing bits using module arithmetic, can be used. Any algorithm can be used, so long as the key is divided unambiguously into components which will be recombined according to some method in order for decryption to proceed. The

multimedia output device 120 then outputs 950 the encrypted content. The multimedia output device 120 also outputs 960 each of the generated fractional keys that are used to decrypt the content. These keys can then be distributed and must be recombined in order for decryption to proceed. This embodiment can be utilized, for example, to provide a facility like a bank safety deposit box, where both a bank manager key and a customer key are required to open the box.

[0093] It should be noted that any of the steps, operations, or processes described herein can be performed or implemented with one or more software modules or hardware modules, alone or in combination with other devices.

Encryption of Audio Data

[0094] As previously described in reference to Fig. 3, output device 120 includes an embedded A/V content recognition module 370 which enables the output device 120 to recognize particular properties in the content and process the data based on the recognized content. Audio data may be represented in several ways. For example, intelligible conversations may be transcribed, and their contents printed out onto paper. In addition, descriptions of audio events along with the time and location of the event can also be depicted on paper. The functionality of A/V content recognition module 370 is described in a co-pending U.S. patent application entitled, "Printing System With Embedded Audio/Video Content Recognition and Processing," to Hull et. al., filed March 30, 2004, Attorney Docket No. 20412-08394, which application is incorporated by reference in its entirety.

[0095] Briefly, a speech recognition processing method is applied to the audio data. The text is printed on a paper document. A representation is provided that indexes the words or phrases that were recognized with high confidence. The print dialog box provides controls for modifying recognition thresholds and layout parameters.

[0096] In one embodiment of the present invention, the functionality of the A/V content recognition module 370 is embedded into the key and metadata generation module 520. Module 520 is adapted to produce various levels of detailed processing of the audio data, in response to a user selection, as described in more details in reference to Fig. 5. For example, module 520 is adapted to produce a transcript of the audio data or high confidence keywords that serve as a memory jog for the creator. In the latter case, the keywords would not reveal the contents of the audio data. As previously discussed in reference to Figs. 2A and 5, a user, for example, selects an option that would print just a key for decrypting the encrypted content. This is the most secure way of outputting decryption information. A user, for example, selects an option that would provide for outputting of a few keywords of the encrypted content. In this case, if the document fell into unauthorized hands, such a printout might provide some clue to the nature of the encrypted data.

Encryption of Video Data

[0097] A/V content recognition module 370 produces various styles of video paper. Video paper is a system for multimedia browsing, analysis, and replay. Briefly, key frames are extracted from video data and printed on paper along with bar codes that allow for random access and reply. Video paper technology is described in "The Video Paper

Multimedia Playback System", Jonathan J. Hull, Berna Erol, Jamey Graham, and Dar-Shyang Lee Ricoh Innovations, Inc. Module 370 is adapted to print one key frame for the whole video file. Alternatively, module 370 prints one key frame per clip. In an alternative embodiment, module 370 prints one key frame per scene. Yet in another embodiment, module 370 prints key frames along with closed caption transcript text. Each of these is adapted to include bar codes to replay the video.

[0098] In one embodiment, the functionality of the A/V module to generate various styles of video paper is embedded into module 520. Module 520 is adapted to produce various levels of detailed processing of the video data, in response to a user selection, as described in more details in reference to Fig. 5. If, for example, a user selected an option that would provide for outputting key frames from video data along with a key, module 520 generates an output that would include the key frames along with the key.

[0099] It should be noted that the key and metadata module 520 is also adapted to generate separate keys for different segments, video clips, speakers, or parts of a recorded meeting (such that one key is generated for video data, one for audio data, one for power point, and one for whiteboard). In addition, some recipients are given the keys selectively for certain parts of the content.

[00100] The foregoing description of the embodiments of the invention has been presented for the purpose of illustration; it is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Persons skilled in the relevant art can appreciate that many modifications and variations are possible in light of the above teachings. It is

therefore intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto.